PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30 — A1

(11) International Publication Number: **WO 96/29795**

(43) International Publication Date: 26 September 1996 (26.09.96)

(21) International Application Number: PCT/US96/03920

(22) International Filing Date: 21 March 1996 (21.03.96)

(30) Priority Data:
08/408,551 21 March 1995 (21.03.95) US

(71)(72) Applicant and Inventor: MICALI, Silvio [US/US]; 459 Chestnut Hill Avenue, Brookline, MA 02146 (US).

(74) Agent: JUDSON, David, H.; Hughes & Luce, L.L.P., Suite 2800, 1717 Main Street, Dallas, TX 75201 (US).

(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SIMULTANEOUS ELECTRONIC TRANSACTIONS

(57) Abstract

A communication method between a first and second party, in the presence of a trusted party, that enables a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party. The method includes two basic steps: exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction, and if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

SIMULTANEOUS ELECTRONIC TRANSACTIONS

TECHNICAL FIELD

The present invention relates generally to electronic commerce and transactions and more particularly to techniques for enabling users to effect certified mail, contract signing and other electronic notarization functions.

BACKGROUND OF THE INVENTION

The value of many transactions depends crucially on their simultaneity. Indeed, simultaneity may be so important to certain financial transactions that entities often are willing to incur great inconvenience and expense to achieve it. For example, consider the situation where two parties have negotiated an important contract that they now intend to "close." Often, the parties find it necessary to sign the document simultaneously, and thus they meet in the same place to watch each other's actions. Another example is the process of certified mail, where ideally the sender of a message desires that the recipient get the message simultaneously with the sender's obtaining a "receipt". A common certified mail procedure requires a person who delivers the mail to personally reach the recipient and obtain a signed acknowledgement when the message is delivered. This acknowledgement is then shipped to the sender. Again, this practice is costly and time consuming. Moreover, such acknowledgements do not indicate the content of the message.

In recent years, the cost, efficiency and convenience of many transactions have been improved tremendously by the availability of electronic networks, such as computer, telephone, fax, broadcasting and others. Yet more recently, digital signatures and public-key encryption have added much needed security to these electronic networks, making such communication channels particularly suitable

for financial transactions. Nevertheless, while electronic communications provide speed, they do not address simultaneity.

The absence of simultaneity from electronic transactions severally limits electronic commerce. In particular, heretofore there has been no effective way of building so-called *simultaneous electronic transactions* ("SET's"). As used herein, a SET is an electronic transaction that is simultaneous at least in a "logically equivalent" way, namely it is guaranteed that certain actions will take place if and only if certain other actions take place. One desirable SET would be certified mail, however, the prior art has not addressed this problem effectively. This can be seen by the following consideration of a hypothetical example, called *extended certified mail* or "ECM".

In an ECM transaction, there is a sender, Alice, who wishes to deliver a given message to an intended recipient, Bob. This delivery should satisfy three main properties. First, if Bob refuses to receive the message (preferably before learning it), then Alice should not get any receipt. Second, if Bob wishes to receive the message, then he will receive it and Alice will get a receipt for the message. Third, Alice's receipt should not be "generic," but closely related to the message itself. Simultaneity is important in this transaction. For instance, Alice's message could be an electronic payment to Bob, and it is desired that she obtains a simultaneous receipt if possible.

Alice could try to get a receipt from Bob of a message m in the following way. Clearly, sending *m* to Bob in the clear as her first communication does not work. Should this message be her digital signature of an electronic payment, a malicious Bob may loose any interest in continuing the conversation so as to deprive Alice of her

receipt. On the other hand, asking Bob to send first a "blind" receipt may not be acceptable to him.

Another alternative is that Alice first sends Bob an encryption of *m*. Second, Bob sends Alice his digital signature of this ciphertext as an "intermediate" receipt. Third, Alice sends him the decryption key. Fourth, Bob sends Alice a receipt for this key. Unfortunately, even this transaction is not secure, because Bob, after learning the message when receiving Alice's key, may refuse to send her any receipt. (On the other hand, one cannot consider Bob's signature of the encrypted message as a valid receipt, because Alice may never send him the decryption key.)

These problems do not disappear by simply adding a few more rounds of communication, typically consisting of "acknowledgements". Usually, such additional rounds make it more difficult to see where the lack of simultaneity lies, but they do not solve the problems.

Various cryptographic approaches exist in the literature that attempt to solve similar problems, but they are not satisfactory in many respects. Some of these methods applicable to multi-party scenarios propose use of verifiable secret sharing (see, for example, Chor et al), or multi-party protocols (as envisioned by Goldreich et al) for making simultaneous some specific transactions between parties. Unfortunately, these methods require a plurality of parties, the majority of which are honest. Thus, they do not envision simultaneous transactions involving only two parties. Indeed, if the majority of two parties are honest then both parties are honest, and thus simultaneity would not be a problem. Moreover, even in a multi-party situation, the complexity of these prior art methods and

their amount and type of communication (typically, they use several rounds of broadcasting), make them generally impractical.

Sophisticated cryptographic transactions between just two parties have been developed but these also are not simultaneous. Indeed, if just two people send each other strings back and forth, and each one of them expects to compute his own result from this conversation, the first to obtain the desired result may stop all communications, thereby depriving the other of his or her result. Nonetheless, attempts at providing simultaneity for two-party transactions have been made, but by using assumptions or methods that are unsatisfactory in various ways.

For example, Blum describes transactions that include contract signing and extended certified mail and that relies on the two parties having roughly equal computing power or knowledge of algorithms. These assumptions, however, do not always hold and are hard to check or enforce anyway. In addition, others have discovered ways to attack this rather complex method. A similar approach to simultaneity has also been proposed by Even Goldreich and Lempel. In another Blum method for achieving simultaneous certified mail, Alice does not know whether she got a valid receipt. She must go to court to determine this, and this is undesirable as well.

A method of Luby et al allows two parties to exchange the decryption of two given ciphertexts in a special way, namely, for both parties the probability that one has to guess correctly the cleartext of the other is slowly increased towards 100%. This method, however, does not enable the parties to achieve guaranteed simultaneity if one party learns the cleartext of the other's ciphertext with absolute probability (e.g., by obtaining the decryption key); then he can deny the other a similar success.

For this reasons several researchers have tried to make simultaneous two-party transactions via the help of one or more external entities, often referred to as "centers", "servers" or "trustees", a notion that appears in a variety of cryptographic contexts (see, for instance, Needham and Schroder and Shamir). A method for simultaneous contract signing and other transactions involving one trustee (called a "judge") has been proposed by Ben-Or et al. Their method relies on an external entity only if one party acts dishonestly, but it does not provide guaranteed simultaneity. In that technique, an honest party is not guaranteed to have a signed contract, even with the help of the external entity. Ben-Or et al only guarantee that the probability that one party gets a signed contract while the other does not is small. The smaller this probability, the more the parties must exchange messages back and forth. In still another method, Rabin envisions transactions with the help of external party that is active at all times (even when no transaction is going on), but also this method does not provide guaranteed simultaneity.

The prior art also suggests abstractly that if one could construct a true simultaneous transaction (e.g., extended certified mail), then the solution thereto might also be useful for constructing other types of electronic transactions (e.g., contract signing). As noted above, however, the art lacks an adequate teaching of how to construct an adequate simultaneous transaction

There has thus been a long-felt need in the art to overcome these and other problems associated with electronic transactions.

BRIEF SUMMARY OF THE INVENTION

It is an object of the invention to provide true simultaneous electronic transactions.

It is a further object of the invention to provide an electronic transaction having guaranteed simultaneity in a two-party scenario and with minimal reliance and support of a third party.

It is another more specific object of the invention to provide simultaneous electronic transactions between two parties that rely on third parties in a minimal and convenient manner. In particular, it is desired to provide electronic transactions between two parties that guarantee simultaneity via the help of an *invisible* third party. A third party is said to be "invisible" because it does not need not to take any action if the transaction occurs with the parties following certain prescribed instructions. Only if one of the original parties deviates from these instructions may the other invoke the intervention of the up-to-then invisible third party, who then can still guarantee the simultaneity of the transaction even though it has not participated from its inception.

These and other objects are provided in a communication method between a first and second party, in the presence of a trusted party, that enables a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party. The method includes two basic steps: exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction, and if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

Where the first party's value is a message and the second party's value is a receipt, the transaction is a certified transmission of

the first party's message. Alternatively, the first party's value represents a commitment to a contract and the second party's value represents a commitment to the contract, such that the transaction is a contract closing.

Preferably, according to the method the first party can prove that some information it receives is the second value, and the second party can prove that some information it receives is the first value.

According to the more specific aspects of the method, at least one of the first and second parties and the trusted party can encrypt messages, and at least one of the first and second parties and the trusted party can decrypt messages. The first set of communications includes at least one communication of the first party to the second party of a data string generated by a process including encrypting a second data string with an encryption key of the trusted party. The second data string includes a ciphertext generated with an encryption key of one of the parties, as well as information specifying or identifying at least one of the parties. The first set of communications also includes at least one communication of the second party of a data string generated by a process that includes having the second party digitally sign a data string computed from information received from the first party in a prior communication, wherein the data string generated by the second party is the second party's value.

According to further aspects of the method, if the second party does not get the first value in the first set of communications, the second party sends the trusted party, for further processing, a data string that includes at least part of the data received from the first party. The further processing by the trusted party includes decrypting a ciphertext with a secret decryption key. The trusted

party then sends the first party information that enables the first party to compute the second value, and the trusted party sends the second party information that enables the second party to compute the first value. In either case, the trusted party also verifies identity information of at least one of the parties but preferably does not learn the first value.

DETAILED DESCRIPTION

In each of the schemes described below, there is a user Alice and a user Bob. The "invisible" third party may be a financial center that facilitates SETs among its customers, including Alice and Bob. For convenience, the following description shows how to make extended certified mail "simultaneous", although the invention is not so limited. In the context of an ECM system, the third party is called the Post Office. As will be seen, however, contrary to ordinary certified mail, the Post Office here is invisible. The inventive scheme is also preferable to ordinary certified mail because the message receipt also guarantees the content of the message. Also, the electronic transaction is faster, more informative and more convenient than traditional certified mail, and its cost should be substantially lower.

In the preferred embodiment, an extended certified mail system is provided using a single "invisible" trustee or "trusted" party. The system is implemented in a computer network, although it should be realized that telephone, fax, broadcast or other communication networks may be used. Thus, without limitation, it is assumed that each user in the system has a computer capable of sending and receiving messages to and from other computers via proper communication channels.

Each user in the system has a unique identifier. Alice's identifier is denoted by A, and Bob's identifier is B. The identifier of the Post Office is denoted by PO. Users and the Post Office can digitally sign messages. Thus, each has a secret signing key and a matching public verification key. If *m* is a message (string), then $SIG_A(m)$ indicates Alice's signature of *m*. (It is assumed, for convenience, that *m* is always retrievable from its signature. This is the case for most signature schemes, and it is otherwise possible to consider a signed message as the pair consisting of the message and its signature.)

Users and the Post Office can encrypt messages by means of a public-key encryption algorithm (e.g., RSA). Thus, each has a public encryption key and a corresponding secret decryption key. $E_A(m)$, $E_B(m)$, and $E_{PO}(m)$ denote, respectively, the encryption of a message *m* with the public key of Alice, Bob, and the Post Office. For simplicity, it is assumed that these schemes are secure in the sense that each of E_A, E_B, and E_{PO} appear to behave as a random function. The system can be suitably modified if these functions are much less secure.

Again, for simplicity these encryption algorithms are deterministic and uniquely decodable. Thus, given a value *y* and a message *m*, all can verify whether *y* is the encryption of *m* with, for example, the Post Office's key, by checking whether $E_{PO}(m)$ equals *y*. (If the encryption scheme is probabilistic, then one may convince another that a string *y* is an encryption of a message m by providing *m* together with the random bits that were used to encrypt *m*.) If *y* is a ciphertext generated by means of the encryption algorithm *E*, $E^{-1}(y)$ denotes the corresponding cleartext, whether or not *E* defines a permutation. (It may also be possible to use encryption algorithms

that are not uniquely decodable, for instance, if it is hard to decrypt a given ciphertext in two different ways.) For simplicity, messages are encrypted directly with a public-key algorithm, however, one could first encrypt a message conventionally with some key *k*, and then encrypt *k* with a public-key algorithm. (Thus, to decrypt *m*, one need only just decrypt *k*).

In one preferred embodiment outlined below, the ECM method requires 5 possible steps of communication: A1 and A2 for user Alice, B1 and B2 for user Bob, and PO for the Post Office. However, at most 3 steps should have to be executed. If Alice and Bob are both honest, only steps A1, B1, and A2 will be executed, and in this order. Step B2 will be executed only if Alice fails to execute Step A2 properly. The execution of Step B2 causes the Post Office to execute its only step, PO. The protocol is as follows:

A1. Given her message *m*, Alice computes $z = E_{PO}((A, B, E_B(m)))$, the encryption in the Post Office public key of a triplet consisting of identifiers A, B and the message m encrypted in Bob's key, and then sends *z* to Bob.

B1. Upon receiving *z* from Alice, Bob digitally signs it and sends it to Alice as the receipt.

A2. If Alice receives the properly signed receipt from Bob, she sends *m* to Bob.

B2. If, within a given interval of time after having executed Step B1, Bob receives a string *m* such that $E_{PO}((A, B, E_B(m))) = z$, the value originally received from Alice, then he outputs *m* as the message and halts. Otherwise, Bob sends the value *z*

signed by him to the Post Office indicating that Alice is the sender and he is the recipient.

PO. If Bob's signature relative to z is correct, the Post Office decrypts z with its secret key. If the result is a triplet consisting of A, B and a string x, the Post Office (a) sends Alice the value z signed by Bob as the receipt, and (b) sends x to Bob.

Preferably, Alice sends z to Bob digitally signed by her. In addition, Alice may sign z in a standard format that indicates z is part of an extended certified mail sent from Alice to Bob, e.g., she may sign the tuple *(ECM, A, B, z)*. In this way, Bob is certain that z comes from Alice and that, when Alice holds a receipt for m signed by Bob, he will have a certified version of m. Further, if z is digitally signed by Alice, Bob first checks Alice's signature, and then countersign z himself. The adoption of a standard format also insures that, by signing z as part of an ECM system, Bob does not sign accidently a message that has been prepared by Alice maliciously. Also, the Post Office may also check Alice's signature or any additional formats if these are used.

In analyzing the protocol, it should be noted that Alice, given Bob's signature of z as receipt, can prove the content of the message by releasing m. Indeed, all can compute $x = E_B(m)$ and then verify that $E_{PO}((A, B, x)) = z$.

Notice also that the Post Office does not understand the message sent via the ECM protocol, whether or not it is called into action. Rather, the Post Office can only obtain $E_B(m)$, but never m in the clear (in this embodiment).

Third, notice that m is, by definition, equal to $E^{-1}_B(x)$, where $(A, B, x) = E_{PO}^{-1}(z)$, and may be non-sensical. Indeed, nothing prevents Alice from sending Bob a garbled message. However, she can only get a receipt for this same garbled message. It is also noted that, if not every string is an encryption of some message, Alice may choose z so that it is not the encryption of anything. In such case, however, she cannot ever claim to have a receipt for any message. Alternatively, it may be desirable to use cryptosystems for which either every string is an encryption of some other string or such that it can be easily detected whether y encrypts something.

The protocol works for the following reasons. When receiving the value $z = E_{PO}((A, B, E_B(m)))$ from Alice, Bob will have difficulty in computing $E_B(m)$, and thus m, from z without the Post Office's secret key. Thus, if he halts, Alice would not get her receipt, but Bob would not get m either.

Assume now that Bob signs z and sends it to Alice. Because this gives Alice a valid receipt from Bob for her message m, for the simultaneity constraint to hold, it must be shown that Bob easily obtains m. This is certainly true if Alice sends m to Bob in Step A1. Assume therefore that Alice does not send him m. Then, Bob presents z signed by him to the Post Office, essentially asking the Post Office to retrieve (for him) $E_B(m)$ from z. The Post Office complies with this request. In doing so, however, the Post Office also sends Alice z signed by Bob as the receipt. It does so to prevent one last possibility; that Bob, upon receiving z from Alice in Step A1, rather than sending her the receipt in Step B1, goes *directly* to the Post Office in order to have $E_B(m)$ extracted from z.

Summarizing, if Alice sends a message encrypted with the Post Office key to Bob, and Bob does not send Alice a receipt, or if

he does not access the Post Office, Bob will never learn *m*. Otherwise, Alice is guaranteed to get her receipt for *m* either from Bob or from the Post Office. On the other hand, upon receiving an encrypted message, Bob is guaranteed that he will understand it, either helped by Alice or helped by the Post Office.

In the preferred embodiment above, the triplet (which includes the ciphertext $E_B(m)$) also includes A and B. The ciphertext is customized in this way so that it can be used by the system only for the purpose of Alice sending a message to Bob. Whether or not this customization is performed, the system is very convenient to use because everyone knows the public key of the Post Office, because everyone can encrypt a value with that key, and because the Post Office can remove this encryption layer for those recipients who claim to have been betrayed by their senders. However, without the above (or an equivalent) customization, this same convenience could be exploited by a malicious recipient, who could learn his messages while denying the senders their legitimate receipts.

In particular, assume that this customization is removed altogether. Then, a malicious Bob, upon receiving $z' = E_{PO}(E_B(m))$ - rather than $z = E_{PO}((A, B, E_B(m)))$ - from Alice in Step A1, may behave as follows. First, he does not send Alice any receipt. Second, he signs z'. Third, he gives this signed value to the Post Office complaining that a sender Chris (an accomplice of his) is refusing to send him the message in the clear. At this point, the Post Office, after verifying Bob's signature and not having any way of checking whether Chris is the real sender, retrieves $E_B(m)$ from z' and sends $E_B(m)$ to Bob, while simultaneously sending the signed z' to Chris as his receipt. Of course, Chris may destroy or hide this receipt. Meanwhile Alice, who does not get any receipt after Step

A1, may think that Bob is away or does not want to receive her message. But she believes that Bob will never be able to read her message in any case.

This violation of the simultaneity constraint (i.e., Bob receiving m while Alice having no receipt) may still occur if, without any customization, Alice signs z when sending it to Bob in Step A1. Indeed, Bob would have no trouble in removing Alice's signature, asking Chris to sign z' and then presenting to the Post Office z' signed by Chris and countersigned by himself. The Post Office, after verifying Bob's and Chris's signatures, would still (after removing its encryption layer) send $E_B(m)$ to Bob and the receipt to Chris. This violation of simultaneity, however, does not occur with the customization of the triplet to include A and B. Indeed, assume that Bob gives the Post Office the value $z = E_{PO}((A, B, E_B(m)))$ originally received by Alice and signed by him and Chris, claiming that it was sent to him by Chris. Then, the Post Office, after verifying Bob's (and Chris's) signature and after computing the value $E_{PO}^{-1}(z)$, will notice that this value - i.e. $(A, B, E_B(m))$ - does not specify Chris to be the sender and Bob the receiver.

The benefits of this customization may be implemented in varying ways. For instance, Alice's signature of $(B,E_B(m))$ may be sufficient to indicate that the sender is Alice and the receiver is Bob. More generally, any customization that prevents Bob from obtaining $E_B(m)$ from the Post Office while convincing the Post Office not to send Alice the receipt is within the scope of the invention.

It should be realized that any customization for the purpose of simultaneous electronic transactions is itself within the scope of the present invention, whether or not implemented with an invisible third party. For instance, Alice may send $E_{PO}(A,B,E_B(m))$ directly to the

Post Office, which gives $E_B(m)$ to Bob (if Bob signs the receipt for Alice) after checking that Alice and Bob are, respectively, the sender and the receiver. Alternatively, Alice may send the Post Office $E_{PO}(SIG_A(B,E_B(m)))$ for identifying the sender and the recipient in a way that cannot be decoupled from the transaction. Such approaches may be especially useful with a plurality of trustees as described below. Such an approach, which calls into action the trusted party directly with a proper customization step as described, is also useful for hiding the identity of the sender from the recipient. Indeed, the Post Office may solicit a proper receipt from Bob without disclosing Alice's identity (even if the receipt indicates the content of Alice's message).

Although not specified above explicitly, it should be appreciated that all or part of the actions required by the Post Office, Alice or Bob can be realized in software. Some of these actions can also be performed by hardware, or physically secure devices (i.e. devices such as secure chips having at least some portion of which is tamper-proof).

Many variations of the disclosed protocol can be envisioned and are within the scope of the present invention. For instance, while the "receipt" described above witnesses the content of the message sent, the receipt can be made generic, e.g., by having Bob sign a "declaration" (instead of a string including an encrypted version of the message) that he has received an encrypted message from Alice at a given time. Also, if desired, the customization step (i.e. the inclusion of the identifiers A and B in the triplet) can be omitted. This might be advantageous, for example, when no other user may collude with either Alice or Bob to disrupt simultaneity. This may occur where there is no third user, as in the case when

certified mail occurs between two predetermined people. In the disclosed system, the Post Office cannot learn the content of the message, but such a restriction can be removed also (e.g., by having Alice compute $z = E_{PO}(A, B, m))$. It may also be convenient to one-way hash strings prior to signing them.

Still another variation would be to impose some temporal element on the transaction. For instance, when Alice sends Bob $z = E_{PO}(A, B, E_B(m))$, she may sign z together with some additional information that specifies a certain time (either absolute or relative to the sending time) after which the Post Office will not help Bob obtain the message. Preferably, Alice specifies this time in a signed manner both outside the Post Office encryption layer as well as within the triplet. In such case, the Post Office must obtain from Bob all necessary information to verify that the time specified outside the PO encryption layer checks with the time specified within the triplet. If it does not, then several possibilities may occur. For example, the Post Office will not help Bob recover the message, or the message is considered unsent (even if Alice obtains a receipt).

Other variations are also possible. Some variations may be used in conjunction or in alternative to the techniques described above. One group of such variants concerns the encryption method used.

For instance, E_B does not need to be interpreted as an encryption algorithm for which Bob has the decryption key. It may just be an encryption algorithm for which Bob can have the message decrypted. For example, and without limitation, the decryption key of E_B may lie with a group of people, each having a piece of the key. These same alternative interpretations apply also to E_A or E_{PO}.

Also, while public-key cryptosystems are quite convenient, it should be realized that conventional cryptosystems could be used for the ECM protocol. For example, x may be the conventional encryption of $(A, B, E_B(m))$ with a secret key k shared between Alice and the Post Office. This key k may be released if it is desired that Bob verify m to be the genuine message. If, however, it is feared that release of a different key may change the content of the messages, special redundancies could be used. For instance, conventionally a message M is encrypted by actually encrypting $(M, H(M))$, where H is a one-way function. Thus, if e is an encryption of $(M, H(M))$ with a key k, it is hard to find a second key K such that e also is an encryption with that key of $(M'H(M'))$. It is preferable that k, rather than being a secret key shared by Alice and the Post Office, is a temporary key that Alice may transfer to the Post Office separately by means of a different shared key K. This way, divulging k (e.g., for the purpose of convincing Bob of the value of $E_B(m)$) does not force the Post Office and Alice to agree on another conventional key k.

It should also be appreciated that the digital signatures of the ECM system need not be public key signatures. For instance, there may be private key digital signatures or signatures verifiable with the help of other parties, or other suitable forms of message authentication. Thus, as used herein, "digital signatures" and "digital signing" should be broadly construed. Similarly, the notion of encryption with a key of some party should be broadly construed to include encrypting with a public key of that party or encrypting with a secret key shared with that party or known to that party.

There may also be concern that the Post Office will collude with one of the parties. For instance, the Post Office may collude

with Bob who, rather than sending the receipt to Alice, goes directly to Post Office, and this enables Bob to understand his message but without giving Alice any receipt. This may occur in ordinary certified mail. Indeed, one who delivers the post may leave a letter with his intended recipient without asking him or her to sign a receipt. Nonetheless, this potential problem may be dealt with effectively and efficiently. For instance, the Post Office may be (or make use of) a physically secure device. Assuming that the Post Office uses such a device in the preferred embodiment, then it will be hard for user Bob to have the Post Office decrypt $(A, B, E_B(m))$ for him without sending Alice her receipt. Indeed, the chip can be programmed to perform both operations or none. Although use of physically secure devices might increase the cost of a system, this need not be the case. Indeed, while they may be millions of users, there may be one or much fewer Post Offices. (Each user, of course, may benefit also from being or relying upon physically secure devices.)

While the inventive ECM system is very economical as it requires at most three communication steps, the goals can be accomplished also by more steps. In particular, although the trusted party, upon receiving Bob's communication, can enable Bob to get his message and Alice to get her receipt, without sending messages back and forth, this goal can be accomplished by means of a more complex dialogue. Indeed, more elaborate dialogues, and in particular zero knowledge proofs (see, e.g., Goldwasser et al or Goldreich et al) could be useful (also as an alternative to physically secure devices) to give Bob the message or Alice the receipt so that they learn their respective values, but are not able to "prove" these values to third parties.

A further alternative method envisions a Post Office with a plurality of trustees. A multiplicity of trustees can be beneficial for various aspects, particularly, if the system is set up so that more than one of the trustees must collude for cheating to occur. Presumably, however, each trustee is selected with trustworthiness (or, if it is a device, proper functioning) as a criterion, and thus the possibility that more than one of them is malicious or defective is very small.

A simultaneous ECM system with a multiplicity of trustees may make novel use of prior techniques such as fair cryptography, or secret sharing, verifiable secret sharing or threshold cryptosystems.

In a construction based on fair public cryptosystems, the triplets $(A, B, E_B(m))$ are not encrypted with the Post Office's public key, but rather with a user public key. In this embodiment, user Alice computes a pair of public and secret key of a fair public-key cryptosystem, properly shares her secret key with the trustees of the Post Office (e.g., receiving from said trustees a certification that they got legitimate shares of this user key) in some initial phase, and then performs Step A1 of the above ECM protocol. If needed, Bob may turn to the Post Office and instructs the trustees to reconstruct Alice's user key. By doing so, the trustees cannot monitor or cause the Post Office to monitor the message addressed by Alice to Bob, but can reconstruct the triplet $(A, B, E(m))$. To insure that the Post Office trustees do not collude with Bob in depriving Alice of her receipt, it can be arranged that each trustee, when contributing its own piece of a user secret key, also gives a proper acknowledgement to that user. Thus, unless all n trustees do not behave properly, Alice would receive at least one receipt.

A possible drawback of this fair-cryptography based system is that Alice must interact with the trustees in order to give them shares of her user key. Thus, the trustees are not fully invisible. This interaction may not even be confined to a single initial phase. This is because Alice may not be able to reuse her key after Bob accesses the Post Office and causes its reconstruction. To alleviate this problem, it might be desirable to use physically secure devices and having the trustees reveal their own pieces to such a device, which would then be able to announce $(A,B,E_B(m))$ without proof.

A better approach uses the ECM protocol, but involves splitting the secret key of the Post Office rather than the secret user keys. Thus, Alice would continue to encrypt $(A, B, E_B(m))$ with the help of the Post Office public key, whose corresponding secret key is shared among the n trustees but is not known to any single entity (nor has it been prepared by any single entity). Thus, the n trustees must cooperate, under Bob's proper request, in removing the Post Office's encryption layer. However, they do so without reconstructing the Post Office secret key, not even internally to the Post Office. To this end, a threshold cryptosystem may be used). This solution is now illustrated using the well- known Diffie-Hellman public-key cryptosystem.

In the Diffie-Hellman system, there is a prime p and a generator g common to all users. A user X chooses his own secret key x at random between 1 and p - 1, and sets his public key to be $g^x \bmod p$. Let y and $g^y \bmod p$, respectively, be the secret and public keys of user Y. Then X and Y essentially share the secret pair key $g^{xy} \bmod p$. Indeed, each of X and Y can compute this pair-key by raising the other's public key to his own secret key mod p. On the other hand, without knowledge of x or y, no other user, given the

public keys g^x mod p and g^y mod p and based on any known method, can compute the pair-key g^{xy}. Thus X and y can use this key to secure communications between each other (e.g., by using it as the key of a symmetric cipher).

Let now $T_1,...,T_n$ be the trustees of the Post Office. Then, each T_i chooses a secret key xi and a matching public key $g^x{}_i$ mod p. Then the public key of the Post Office is set to be the product of these public keys mod p, g^z mod p (i.e., $g^z = g^{x1+...+xn}$ *mod* p). Thus, each trustee has a share of the corresponding secret key, z. Indeed, the Post Office's secret key would be $z = x1 +... +xn$ mod p - 1. Assume now that Alice wishes to encrypt *(A, B,* $E_B(m)$*)* with the Post Office's key. She selects a (preferably) temporary secret key a and its corresponding public key g^a mod p. She then computes the public pair-key g^{az} mod p, encrypts *(A, B,* $E_B(m)$*)* conventionally with the secret pair-key g^{az}, and then sends Bob this ciphertext together with the temporary public-key g^a mod p (all in Step A1). If in Step B1 Bob sends Alice back a receipt, namely, his signature of the received message, then Alice, in Step A2, sends him the secret key a. This enables Bob to compute the pair-key g^{az} mod p (from a and the Post Office's public key), and thus decrypt the conventional ciphertext to obtain *(A, B,* $E_B(m)$*)*. Thus, if both users behave properly, the Post Office is not involved in the transaction. Assume now that Bob properly asks the Post Office to decrypt Alice's ciphertext. To do this, the trustees cooperate (preferably, with proper notice to Alice and to each other) in computing g^{az} mod p. To this end, each trustee T_i raises Alice's public key g^a mod p to its own secret key. That is, T_i computes g^{axi} mod p. Then these shares of the pair-key are multiplied together mod p to obtain the desired private pair-key. In fact, $g^{ax1}...g^{axn}$ mod $p = g^{ax1+...+axn}$ mod $p = g^{a(x1+...+xn)}$ mod $p = g^{az}$

mod p. This key may be given to Bob, who can thus obtain $E_B(m)$. In this method, it may be useful to have a Post Office representative handle the communications with Bob, while the individual trustees handle directly their sending Alice receipts.

This method can be adjusted so that sufficiently few (alternatively, certain groups of) trustees cannot remove the Post Office's encryption layer, while sufficiently many (alternatively, certain other groups of) trustees can. For instance, there can be kn trustees, and each of the n trustees acting as above can give his own secret key to each of a group of k - 1 other trustees. Thus, each distinct group of k trustees has knowledge of a secret key as above. Further, the above-described modifications to the single invisible-trustee ECM protocol can be applied to embodiments involving multiple trustees.

In the ECM system involving fair cryptography, even a user might be or rely upon a multiplicity of entities. Indeed, in the invention, "user" or "party" or "trusted party" thus should be construed broadly to include this possibility.

It should be appreciated that the inventive ECM systems enable Alice and Bob to exchange simultaneously two special values, the first, produced by Alice, which is (at least reasonably) unpredictable to Bob, and the second, produced by Bob, which is unpredictable to Alice. Indeed, the value produced by Bob and unpredictable to Alice may be Bob's signature of step B1. If the message is not known precisely by Bob, then the message itself may be the value produced by Alice and unpredictable to Bob. Alternatively, if Bob knows the message precisely (but it is desired that he receive it from Alice in an official and certified manner), then the parties may use a customization step so that, for example

$SIG_A(m,E_B(m))$ is the value produced by Alice and unpredictable to Bob.

The inventive system is useful to facilitate other electronic transactions that require the simultaneous exchange of unpredictable values. One such example, not meant to be limiting, involves a contract "closing" wherein a pair of users desire to sign a contract at a particular time and place. The invention thus allows Alice and Bob to sign a contract simultaneously with an invisible third party. Indeed, the first value may be Alice's signature of the contract C and the second value Bob's receipt for a message consisting of Alice's signature of C.

In particular, assume that Alice and Bob have already negotiated a contract C. Then, Alice and Bob agree (in a preliminary agreement) (a) that Alice is committed to C if Bob gets the message consisting of Alice's signature to C, and (b) that Bob is committed to C if Alice gets Bob's receipt of that message. This preliminary agreement can be "sealed" in many ways, for instance by signing, preferably standardized, statements to this effect conventionally or digitally. It does not matter who signs this preliminary agreement first because Bob does not have Alice's message and Alice does not have Bob's receipt. However, after both parties are committed to the preliminary agreement, the inventive ECM system allows the message and the receipt to be exchanged simultaneously, and thus C is signed simultaneously. Those skilled in the art also may realize it may be more convenient to first one-way hash C prior to signing it.

This method may be much more practical than accessing a commonly trusted lawyer particularly, when the contract in question may be very elementary or arises in an "automatic context". Generalizing, one may view a contract C as any arbitrary signal or

string of symbols to which the parties wish to commit in a simultaneous way. The inventive solution is very attractive because it can be implemented in software in many contexts, and because the trustee is invisible and need not be called into use if the signatories behave properly. This minimizes cost and time, among other resources. In this application, the trustee, rather than a post office, may be a "financial service center" that facilitates the transactions of its own customers.

Yet another application of the invention is to make simultaneous the result of applying a given function to one or more secret values, some belonging to Alice and some belonging to Bob. For example, the inventive method allows implementation of "blind" negotiations. In this embodiment, assume a seller Alice and a buyer Bob desire to determine whether Alice's (secret) minimum selling price is lower than Bob's (secret) maximum selling price (in a way that both parties will learn the result simultaneously). If the answer is no, then the parties may either try again or terminate the negotiation. Alternatively, if the answer is yes, then preferably the parties also will be committed to the transaction at some value. (For example, the average of the two secret values).

Another useful application of the invention is during a bid process, such as in an auction. For instance, assume that multiple bidders wish that their secret bids be revealed simultaneously. One bidder may also wish that his or her bid be independent of the other bids.

CLAIMS:

What is claimed is:

1. A communication method between a first and second party, in the presence of a trusted party, enabling a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party, comprising the steps of:

exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction; and

If the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

2. The communication method as described in Claim 1 wherein the first party's value is a message and the second party's value is a receipt, such that the transaction is a certified transmission of the first party's message.

3. The communication method as described in Claim 1 wherein the first party can prove that some information it receives is the second value.

4. The communication method as described in Claim 1 wherein the second party can prove that some information it receives is the first value.

5. The communication method as described in Claim 1 wherein the first party can prove that some information it receives is the second value and the second party can prove that some information it receives is the first value.

6. The communication method as described in Claim 1 wherein the first party's value represents a commitment to a contract and the second party's value represents a commitment to the contract, such that the transaction is a contract closing.

7. The communication method as described in Claim 6 wherein the first party can prove that some information it receives is the second value and the second party can prove that some information it receives is the first value.

8. The communication method as described in Claim 1 wherein at least one of the first and second parties and the trusted party can encrypt messages, and at least one of the first and second parties and the trusted party can decrypt messages.

9. The communication method as described in Claim 8 wherein at least one communication of the first party is a data string generated by a process including encrypting a second data string with an encryption key of the trusted party.

10. The communication method as described in Claim 9 wherein the second data string includes a ciphertext generated with an encryption key of one of the parties.

11. The communication method as described in Claim 9 wherein the second data string contains information identifying at least one of the parties.

12. The communication method as described in Claim 8 wherein at least one communication of the second party is a data string generated by a process that includes having the second party digitally sign a data string computed from information received from the first party in a prior communication, wherein the data string generated by the second party is the second party's value.

13. The communication method as described in Claim 8 wherein if the second party does not get the first value in the first set of communications, the second party sends the trusted party for further processing a data string that 5 includes at least part of the data received from the first party.

14. The communication method as described in Claim 13 wherein the further processing by the trusted party includes decrypting a ciphertext with a secret decryption key.

15. The communication method as described in Claim 14 wherein the trusted party sends the first party information that enables the first party to compute the second value, and the trusted party sends the second party information that enables the second party to compute the first value.

16. The communication method as described in Claim 15 wherein the trusted party also verifies identity information of at least one of the parties and does not learn the first value.

17. The communication method as described in Claim 1 wherein the trusted party takes no action to complete the transaction after a specified time.

18. The communication method as described in Claim 17 wherein the specified time is included within the first set of communications.

19. The communication method as described in Claim 17 wherein the specified time is determined by the time at which certain communications occur.

20. A method by which first and second parties and a trusted party effect a certified mail transaction, each of the parties having matching public and secret keys of a public key encryption scheme, and wherein the first party desires to send a message to the second party and obtain a message receipt indicating the content of the message to thereby complete the certified mail transaction, comprising the steps of:

(a) having the first party generate and send to the second party a data string including an encryption, with the trusted party's public key, of information that prevents the trusted party for enabling the second party to obtain the first party's message without the first party obtaining the message receipt;

(b) upon receipt by the second party of the data string, having the second party generate and send to the first party the message receipt;

(c) upon receipt by the first party of the message receipt, having the first party send to the second party information that enables the second party to retrieve the 20message;

(d) upon receipt by the second party of the information, having the second party attempt to verify whether the message was received; and

(e) if the message was not received, having the second party send information to the trusted party for further processing, wherein the information includes a ciphertext encrypted with a public key of the trusted party.

21. The method as described in Claim 20 further including the step of:

(f) having the trusted party, using the information received from the second party, (i) decrypt some information it receives from the second party using the secret key of its public key encryption scheme to thereby generate an encryption of the first party's message using the second party's public key, and (ii) obtain information that identifies at least the first party.

22. The method as described in Claim 21 further including the unordered steps of;

(g) having the trusted party send the first party, as the message receipt, some of the information the trusted party received from the second party; and

(h) having the trusted party send the second party information from which the second party can retrieve the message.

23. The method as described in Claim 20 wherein at least one of the first and second parties and the trusted party includes a physically secure device.

24. The communication method as described in Claim 20 wherein further processing by the trusted party does not occur after a specified time.

25. The communication method as described in Claim 24 wherein the specified time is included within at least communication between the first and second parties.

26. The communication method as described in Claim 24 wherein the specified time is determined by the time at which certain communications occur.

27. A communication method between a first and second party, in the presence of a plurality of trustees, enabling a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party, comprising the steps of:

exchanging a first set of communications between the first and second parties without participation of any of the trustees to attempt completion of the transaction; and if the transaction is not completed using the first set of communications between the first

and second parties, having a given number of the trustees take action to complete the transaction.

28. The communication method as described in Claim 27 wherein the plurality of trustees hold shares of a given secret key.

29. The communication method as described in Claim 27 wherein at least one of the first and second parties and the trusted party can encrypt messages, and at least one of the first and second parties and the trusted party can decrypt messages.

30. The communication method as described in Claim 27 wherein at least one communication of the second party is a data string generated by a process that includes having the second party digitally sign a data string computed from information received from the first party in a prior communication, wherein the data string generated by the second party is the second party's value.

31. The communication method as described in Claim 30 wherein if the second party does not get the first value in the first set of communications, the second party sends the trusted party for further processing a data string that includes at least part of the data received from the first party.

32. The communication method as described in Claim 27 wherein the trusted party takes no action to complete the transaction after a specified time.

33. The communication method as described in Claim 32 wherein the specified time is included within the first set of communications.

34. The communication method as described in Claim 32 wherein the specified time is determined by the time at which certain communications occur.

35. In a communications network wherein first and second parties desire to effect a transaction overseen by a trusted party of the network, each of the first and second parties having a value that cannot be predicted by the other of the first and second parties, and wherein the predetermined transaction is complete when the first party receives the value generated by the second party and the second party receives the value generated by the first party, a communication method comprising the steps of:

exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction; and

if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

36. In the communications network as described in Claim 35 wherein at least one of the first and second parties is a computer.

37. In the communications network as described in Claim 35 wherein the trusted party is a computer.

38. In the communications network as described in Claim 35 wherein at least one of the first and second parties is a secure device.

39. A communication method between a first and second party enabling a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party, comprising the steps of:

having the first party use a key of a third party to encrypt a string from which the second party can compute the first value; and having the first, second and third parties exchange a set of communications that include the string.

40. The method as described in Claim 39 wherein the string also includes information that is selected from the group consisting of information specifying the first party, information specifying the second party, and information specifying the first and second parties.

41. The method as described in Claim 39 wherein the key of the third party is held by a plurality of trustees.

42. The method as described in Claim 39 wherein the first party comprises a plurality of entities.

43. The method as described in Claim 39 wherein the second party comprises a plurality of entities.

44. The communication method as described in Claim 39 wherein at least one of the parties takes no action to complete the transaction after a specified time.

45. The communication method as described in Claim 44 wherein the specified time is specified by at least one of the parties.

46. The communication method as described in Claim 44 wherein the specified time is determined by the time at which certain communications are received.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03920

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/30
US CL :380/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,438,824 (MUELLER-SCHLOER) 27 March 1984, See entire document.	9-17, 20-26, 30, 31, 37
Y	US, A, 4,458,109 (MUELLER-SCHLOER) 03 July 1984, See entire document.	9-17, 20-26, 30, 31, 37
Y	US, A, 5,214,700 (PINKAS ET AL) 25 May 1993 See Figs. 2 and 4.	9-17, 20-26, 30, 31, 37
Y	US, A, 5,276,737 (MICALI) 04 January 1994, See Fig. 2.	9-17, 20-26, 30, 31, 37
Y	US, A, 5,315,658 (MICALI) 24 May 1994, See Fig. 2.	9-17, 20-26, 30, 31, 37

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 JUNE 1996	Date of mailing of the international search report 02 AUG 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer for SALVATORE CANGIALOSI Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03920

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 1-8, 17-19, 27-29, 32-35, 38-46
because they relate to subject matter not required to be searched by this Authority, namely:

They disclose a method of doing business which is not embodied in any specific means.

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.